



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|----------------------|---------------------|------------------|
|-----------------|-------------|----------------------|---------------------|------------------|

09/720,353

12/21/2000

Michael Nolte

6400-11WOUS

1134

7590

01/30/2006

McCormick Paulding & Huber
City Place II
185 Asylum Street
Hartford, CT 06103-4102

EXAMINER

POLTORAK, PIOTR

ART UNIT

PAPER NUMBER

2134

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/720,353

Applicant(s)

NOLTE, MICHAEL

Examiner

Peter Poltorak

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 05 October 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☒ Claim(s) 17 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

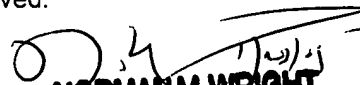
Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☒ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.


NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____

DETAILED ACTION

1. Claims 2-17 have been examined.

PriorityForeign priority has been claimed in this application.

3. Acknowledgment is made of applicant's claim for foreign priority based on an application filed in Germany on 4/30/1999. It is noted, however, that applicant **has not filed a certified copy of the German application** as required by 35 U.S.C. 119(b).
4. The effective priority date for the subject matter in the pending claims in this application once the paper has been received will be 4/30/1999.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

5. Claims 2-17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.
6. Claim 11 recites: "the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message". The specification discloses taking a pair of sequence numbers and signing keys and using the signer to determine the signature for the message" (pg. 5 lines 31-35). However, claim 11

continues: "using the check key and the determined sequence number to form a calculated signature" but the specification suggests that the check key is passed to a signature checker together with the message to verify the signature (*pg. 6 lines 29-35*). Although the specification recites "the sequence number" it fails short of teaching "using the check key and determined sequence number to form a calculated signature".

7. Claim 9 comprising the limitation: "the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block" is similarly rejected.
8. Claim 13 recites: "when a data set is received at the receiver, producing a new value of the sequence number". Even though the specification discloses "these pseudo-random number generators produce a sequence of new numbers in each case until the cycle ..." it fails short of disclosing that a new value is produced when a data set is received at the receiver.
9. Claims 2-8, 12, 14-17 are rejected by virtue of their dependence.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

10. Claims 2-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.

Art Unit: 2134

11. As discussed above claim 11 recites: “the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message”.

The specification discloses taking a pair of sequence numbers and signing keys and using the signer to determine the signature for the message” (*pg. 5 lines 31-35*).

However, claim 11 continues: “using the check key and the determined sequence number to form a calculated signature” but the specification suggests that the check key is passed to a signature checker together with the message to verify the signature (*pg. 6 lines 29-35*). Although the specification recites “the sequence number” it fail short of teaching “using the check key and determined sequence number to form a calculated signature”.

12. It is not clear whether there is a problem with the written description, or understanding of the specification and claim language.

13. The specification suggests that method relating to creation of signatures has been described frequently and comprehensively in the cryptographic literature (*pg. 5 lines 34 – pg. 6 line 6*). In the literature, the same set of data (*or at least corresponding set of data if public cryptography is used*) is used in the signature verification as in the signature creation (*e.g. Stallings, pg. 247-249*).

14. For purposes of further examination and in light of the supporting drawing the limitation “the sender using the at least one pair of the signing key and the selected sequence number to form a signature for a message” is treated as “the sender using the at least one pair of the signing key and the selected sequence number to form a

data set that contains a signature for a message *(the specification pg. 6 lines 8-11 and the middle part (referring to the sender 20) of the Fig. 1).*

15. The limitation: "using the check key and the determined sequence number to form a calculated signature" is treated as using the check key that is derived from the determined sequence number in forming a calculated signature.

16. Similarly, the recitation: "the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block" is treated as "the check key and the determined sequence number being used to derive the check key that is used in forming a calculated signature for comparison to the signature of the data message block".

17. Claim 9 discloses a similar problem ("the check key and the determined sequence number being used to form a calculated signature for comparison to the signature of the data message block") and is similarly rejected.

18. Claim 13 recites: "when a data set is received at the receiver, producing a new value of the sequence number". It is not clear whether the limitation is directed to the control center that creates a new value of the sequence number and if it is so the meaning of "when" is not clear. It is not clear whether as soon as the data set reaches the receiver a new value is created, whether the control center waits for the response etc. Perhaps the limitation is directed to the sender receiving the data set upon which the sender retrieves (generate) a new value of the sequence number for the received data. For purposes of further examination the phrase is treated as best understood.

19. Claims 2-8, 12, 14-17 are rejected by virtue of their dependence.

Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

20. Claims 2-7, 9, 11-13 and 16 are rejected under 35 U.S.C. 102(b) as being

anticipated by *Hoffmann et al.* (U.S. Patent No. 5608800).

21. As per claim 11 *Hoffmann et al.* teach a control center producing one or more

sequence numbers (*random data Z*), and using one of the sequence numbers and the common main key (*coupling data K*) creating a signing key (*symmetric key E*) by means of one-time encryption (*col. 3 lines 37-43*). The signing key and the sequence number is provided to the sender via a secure transmission (a control center and a sender are both within a transmitter) and the sender using the signing key forms a signature for a message (*col. 1 lines 44-46 and col. 3 lines 19-22*).

Furthermore *Hoffman et al.* teach a control center sharing undiscoverable main key with a receiver as well as sending the message to the receiver via a data set containing at least the message and the (*enciphered*) signature (*S/E*) (*col. 3 lines 45-52*). *Hoffman et al.* teach determining the sequence number from the received data

Art Unit: 2134

set (*col. 3 lines 65-67*), passing the sequence number through a one-time encryption to produce a check key (*col. 4 lines 1-3*) and using the check key to verify the signature of the message (*col. 4 lines 4-7*).

22. *Hoffman et al.* teach the limitation of claim 5 in *col. 3 lines 37-38*.

23. Claims 2-7 and 9 are substantially equivalent to the limitations of claim 11; therefore claims 2-7 and 9 are similarly rejected.

24. As per claims 13 and 16 the pseudo-random number generator must have an initial value in order to provide any output. Also, since the pseudo-random number generator creates a new value whenever a message is to be transmitted a new value is created (*col. 3 lines 34-53*). Furthermore, as discussed above the same input must be used in creation of a signature (in non public key cryptography) in order for the signature integrity be verified.

Claim Rejections - 35 USC § 103

25. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

26. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (*U.S. Patent No. 5608800*) in view of *Horstmann* (*U.S. Patent No 6009401*).

27. As per claim 8 *Hoffmann et al.* teach the receiver as discussed above. *Hoffmann et al.* does not explicitly teach the receiver maintaining a list of already used sequence

Art Unit: 2134

numbers, and rejects already used sequence numbers. *Horstmann et al.* teach a receiver (*the clearinghouse*) maintaining a list of already used sequence numbers (*used tickets*) and rejects already used sequence numbers (*Horstmann et al.*, col. 5 lines 21-27).

28. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to maintain a list of already used sequence numbers by a receiver and reject already used sequence numbers as taught by *Horstmann et al.*. One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid a replay attacks (*Horstmann et al.*, col. 5 line 22-23).

29. Claims 10 and 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (U.S. Patent No. 5608800) in view of *Official Notice*.

30. *Hoffmann et al.* teach random number generator as discussed above.

31. *Hoffmann et al.* do not teach the generator producing a sequence number using a deterministic method.

Official Notice is taken that it is old and well-known practice to use deterministic methods to produce numbers. One of ordinary skill in art at the time of applicant's invention would employ deterministic method number generation in order to have control over number generation wherein given the same input the same output could be generated.

32. *Hoffmann et al.* also do not teach storing signing key and the selected sequence number in a smart card.

Art Unit: 2134


33. Official Notice is taken that it is old and well-known practice to use smart card to store (and transport) secure information such as signing keys and corresponding sequence numbers. One of ordinary skill in the art at the time of applicant's invention would have been motivated to use smart card to store signing keys and selected sequence numbers given benefit of security as well as convenience and portability.
34. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over *Hoffmann et al.* (U.S. Patent No. 5608800) in view of *Hoffman et al.* (U.S. Patent No. 5613012).
35. *Hoffmann et al.* teach the sequence number as discussed above.
36. *Hoffmann et al.* do not teach that the sequence number comprise of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing a data and time, the time including a number of seconds from an appointed start time.
37. *Hoffman et al.* '5613012 teach that the sequence number comprise of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing a data and time, the time including a number of seconds from an appointed start time (col. 97 lines 45-49).
38. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include the sequence number comprise of one of decreasing numbers, numbers with a step interval greater than unity and numbers representing a data and time, the time including a number of seconds from an appointed start time. One of ordinary skill in the art would have been motivated to perform such a modification in order to easily identify each transmission.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


1/9/06


1/23/05
NORMAN M. WRIGHT
PRIMARY EXAMINER